Guidelines

For

Technical and Financial Support

For

Establishment of State Data Centre (SDC)

Department of Information Technology,
Govt. of India, Electronics Niketan,
New Delhi – 110 003.

1.0 Preamble

1.1 State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of NeGP. Under NeGP, it is proposed to create State Data Centres for the States to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. These services can be rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as State Wide Area Network (SWAN) and Common Service Centre (CSC) connectivity extended up to village level. State Data Centre would provide many functionalities and some of the key functionalities are Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration.

2.0 Background

2.1 The State Data Centre is a key-supporting element of e-Government Initiatives & businesses for delivering services to the citizens with greater reliability, availability and serviceability. SDC provides better operations & management control and minimizes overall cost of Data Management, IT Management, Deployment and other costs.

2.2 State Data Centre acts as a mediator and convergence point between open unsecured public domain and sensitive government environment. It enables various State departments to host their services/applications on a common infrastructure leading to ease of integration and efficient management, ensuring that computing resources and the support connectivity infrastructure (SWAN/NICNET) is adequately and optimally used.

2.3 The design of Data Centre represents many challenges and is a complex task as it involves many stakeholders (state departments having varying

requirements, access mechanism and delivery channels to the citizens). The extent to which the SDC must remain operational even when some of its resources are impaired or unavailable will greatly influence how the design objectives of Reliability, Availability, Scalability, Serviceability and also Backup, Redundancy, Survivability and Disaster Management are met.

The SDC will be equipped to host / co-locate systems (e.g. Web Servers, Application Servers, Database Servers, SAN, and NAS etc.) to host applications at the SDC to use the centralized computing power. The centralized computers/Servers will be used to host multiple applications. SDC will have high availability, centralized authenticating system to authenticate the users to access their respective systems depending on the authentication matrix.

2.4 Department of Information Technology (DIT) has taken note of the broad requirements for a typical data centre which include infrastructure facilities (physical, electrical, air conditioning etc.,) installation and integration of IT infrastructure (servers, telecom equipment, integrated portal/ departmental information system, Enterprise and network management system, security, firewalls/IDS, networking components etc.), software and databases. Establishing a State Data Centre is a complex task and requires substantial investment and efficient Operations and Management. Therefore it may be prudent to utilize the services of existing IDC players in the country with due and adequate security and policy measures/considerations. The paramount consideration in any arrangement is the security of the data and the preservation of the ownership and control of government data, both de jure and de facto.

3.0 In view of the above, DIT has formulated the Guidelines to provide Technical and Financial assistance to the States for setting up State Data Centre. These Guidelines also include the norms for outsourcing of the SDC to a private/ public sector service provider including some of the technical and administrative

norms to be followed by the States, depending on the implementation option adopted by the State to establish the SDC.

3.1 While formulating the Guidelines, DIT has noted that some State Governments would have different approach to State Data Centre while hosting applications at the SDC. In case States are using repository of Servers at the District level, the SDC in such case may act as a central repository for consolidation of the disaggregated resources.

3.2 Department of IT has also taken note of the proliferation/size of applications to be hosted at the SDC and has built-in provisions to ensure future scalability of the SDC while determining its initial sizing.

3.3 For the purpose of the sizing of the State Data Centre, the States have been put in three categories of Large, Medium and Small based on the population/ number of districts in each State.

4.0 Implementation Options

4.1 State would need to establish the SDC using any one of the two options indicated below:

Option I: State/UT and NIC together form a composite team for the State Data Centre. While sovereign control of the data/ applications shall be with the State (both de- jure and de-facto); NIC through its dedicated core team (6-7 domain experts /professionals) which may be specially created for each State, shall provide complete handholding for infrastructure up-keep, operations & management including issues related to business continuity. NIC Data Centre team would further be supported by domain specialists and support staff that would to be recruited by the Centre/State for the State Data Centre. The Facility Management services for physical infrastructure may be outsourced, if required.

However, for this option a tightly coupled administrative and techno-functional arrangement with clear roles and responsibilities of both the State IT department and State NIC Data Centre team shall be put in place and implemented. The Data Centre administrative responsibility shall be with State IT Secretary, the technical and day to day operations shall be the responsibility of the designated NIC Data Centre Project Manager. While the Project Manager shall functionally report to State IT Secretary; for all matters related to State NIC team, he/she shall report to DG NIC.

In case of any issues involving higher level intervention, an Apex Committee chaired by the Chief Secretary of the State with DG-NIC as co-chairman is suggested. Other members of the committee shall be State IT secretary, NIC Project Manager and a representative from DIT.

Template RFP for this option shall be made available to the States including a consulting agency by DIT. The consultancy agency would assist the States for project development (DPR), bid process management, supervision and overall implementation of the State Data Centre.

Option II : The State/UT leverages the capabilities of existing commercial Internet Data Centres (IDCs) for which different deployment models are available i.e. Co-located services, Dedicated Services and Managed Services. Under this option, the State may identify a suitable model (confined to either co-located services or dedicated services only keeping in view the security implications) to select an appropriate agency through a suitable competitive process for outsourcing. The entire process of outsourcing, including advising on the most appropriate model, would be managed by the consulting agency to be made available by DIT to the State. Template RFP for this option shall be made available to the States by DIT. Depending upon whatever outsourced model is selected by the State, Servers will be owned and operated by State and the management of the Data/Information shall be under the direct control of the State both de-jure and de-facto. For this, the State would require to deploy a dedicated

team which includes Project Manager (equivalent to Data Centre Manager), DBA, System administrator, Network Administrator, Support Staff etc as broadly indicated at Annexure 4 of the policy guidelines. Further, the State may also exercise the option to engage and utilize the manpower resources of NIC. States would not be permitted to choose implementation Option- II unless one of the following two criteria is met:

i. The Core Data Centre team is headed by a Project Manager drawn from the NIC. For this arrangement a mutual agreement between the State Government and NIC shall be worked out.

OR

ii. The State Government would have to satisfy the DIT/Empowered Committee set up by DIT, regarding their technical competence and ability to handle the security issues involved adequately, while hosting their Data/Applications in a commercial IDC.

For both Option I & II, the State would need to designate an appropriate Central/ State agency to take overall responsibility for receipt of funding support, implementation and rendering accounts/ Utilization Certificates.

Whatever options as above that may be exercised by the States, necessary Service Level Agreement would be defined and SLAs finalized. An implementation committee shall be constituted by the State with a representative from DIT and State NIC as members of the committee.

4.2 Depending upon whatever option as above is adopted by the State, the essential requirements as regards physical security, access mechanism, data protection and security, confidentiality, privacy issues and business continuity plan would need to be complied with, by the State in view of the sovereignty /sensitivity of the databases and the applications hosted in the SDC. These have been attached at Annexure -1 & 2 to the Guidelines to

help/guide the State. Further, the stipulations/standards on data security, computing environment and storage environment have also been elaborated at Annexure -3 for the benefit of the State.

5.0 Eligibility Conditions for States for DIT funding support.

5.1 States should have initiated action for setting up of SWAN, which shall provide connectivity between the proposed Data Centre site, and the Secretariat ,various Departments and at District and Block level, wherever, required.

5.2 The State would need to have undertaken implementation of at least three major statewide e-governance projects/services/applications that require creation of SDC of which at least one should have been completed in order to be eligible for funding support.

6.0 Norms for Sharing of Cost between GoI and State Govts.

6.1 GoI support will cover the entire cost of establishment, operation and maintenance of the State Data Centre for a period of five years on 100% grant-in-aid basis. The financial assistance being provided to the States shall include refurbishing of the physical space to the Data Centre requirements including back-up power supply (UPS and DG sets) and Air-Conditioning requirements. The cost of consultancy for option I and consultancy for undertaking technical feasibility study, advising on most appropriate model, preparation of SLA, etc. in case of Option II, will be provided as 100% grant by DIT to the agency designated by the State to undertake the selection of the IDC service provider. The cost of monitoring of performance under SLAs would also be covered by GoI support, including cost of engaging a third party for such monitoring/audit of the SDC.

6.2 The cost of manpower required for domain specialist team for Data Centre operations & management over a period of 5 years shall be provided by the GoI.

6.3 For planning purposes, the sizing of the Data Centre has been classified in three categories: Large, Medium and Small which shall also depend upon the number of applications and the data size. Accordingly, the funding to the States may vary with adequate provision built-in, for upgradation/scaling of the Data Centre during the initial period of 5 years.

7.0 Exclusions from DIT funding support

7.1 The physical space required for the Data Centre would be the responsibility of the State. A well secured area for the SDC would be demarcated. The demarcated area should have readily available power connection preferably from two different sources, water connection and other civic amenities.

7.2 The Back-End computerization of the Deptts would be the responsibility of the State and no financial support is envisaged in this regard as part of State Data Centre.

7.3 The cost of providing connectivity to the State Data Centre would be outside the scope of the Data Centre. The State can connect the Data Centre to the State PoPs, which is being provided by the DIT as part of SWAN scheme.

7.4 The cost of providing connectivity to the Disaster Recovery from the Primary Data Centre Site and the Internet bandwidth required at the Primary & DR site would be outside the scope of the Data Centre Scheme and shall be borne by the State.

7.5 Any incremental investment beyond 5 years period would be the responsibility of the State.

8.0 Deployment Architecture for delivery mechanism

8.1 The architecture of a Data Centre would be such as to provide a model environment capable of handling the typical business model of dynamic change supporting multiple G2G, G2C, G2B, B2C activities across all channels like CSCs, portals, kiosks etc. As e-Governance applications are expected to grow, the Data Centre architecture shall be highly scalable and be built on a solid architectural foundation. The power and cooling system should at least meet with Tier-I requirements with possibility of upgrading to the next level. The State Data Centre Architecture would be multi-layered architecture and the applications to be hosted in the Data Centre shall support interoperability standards like XML, SOAP etc. The State Data Centre would provide infrastructure such as firewall service, directory service, web service, database service, portal, integration, management, data storage services and possibly a standards based messaging Gateway, which could be a shared infrastructure to all the applications / departments in the State Data Centre.

9.0 Data Centre Management and Monitoring

9.1 A centralized management and monitoring system (tool) capable of doing fault management, configuration management, security management, report generation, alerting, monitoring the critical servers, log monitoring and Data Centre network and security infrastructure etc. would be part of the Data Centre. This system/tool would be scalable as well as be able to provide a hierarchical troubleshooting. In case, the Enterprise Management and Monitoring tool is already available for SWAN, the same would be utilized for State Data Centre requirements as well.

10.0 Service Availability & its Monitoring

10.1 End-to-end service availability of the SDC and its independent monitoring is the prime requirement to have reliable, seamless, smooth delivery of the services

to the citizens and other G2G & G2B applications meeting the objectives of this core e-Governance infrastructure. It is, therefore, necessary that appropriate Service Level Agreements (SLAs) be worked out between the States and the Implementing Agency and that an Independent Agency would be appointed to monitor the performance with reference to the SLA and related aspects.

11.0 Disaster Recovery and Business Continuity Plan

11.1 The high availability is one of the critical requirements of the Data Centre. As the systems are centralized at Data Centre, the State would be required to establish appropriate Disaster Recovery and Business Continuity Plan (DR and BCP) along with appropriate data backup and recovery infrastructure. Initially, State should plan for off-site Back-up mechanism for their DR strategy and depending upon mission critical requirement the BCP requirement would be met through the design architecture of the primary Data Centre itself.

The Disaster Recovery (DR) arrangement has been envisaged to be established and provided by NIC. NIC is in the process of setting up National Data Centres at Hyderabad and Pune of the order of 8000 sq. ft. each, apart from existing National Data Centre at Delhi. These centres will be connected through high speed networks to support data/application back-up facility and likely to be operational within one year time frame. While these centres will house largely central government data, these would have enough capacity to be used as DRs for the SDCs on a regional basis. One more Data Centre to take care of the Eastern region is planned to be setup by NIC at Bhubaneswar for which a budget provision over 5 years period has been included in the SDC scheme outlay.

12.0 Data Retention Plan

12.1 The State would formulate an appropriate Data Retention policy and ensure that the data centre architecture supports the same. The Data Retention Policy would be guided by the following factors:

a. Data classification and risk assessment of data.

b. Data Retention Period.

c. Data Security aspects.

d. Disposal of data once the retention period is over.

13.0 Data Centre Protection

13.1 The data centre shall have the required protection and safeguard mechanism for physical security, network security and facility infrastructure requirements including protection against fire, natural calamity and man made risks.

14.0 Security Audit

14.1 The State shall get the security audited by third party expert periodically (once in six months) and as and when there is significant upgradation of systems which include hardware, software and network resources to ensure and guarantee security of the Data Centre. The audit shall bring out any security lapses in the system and establish that the system is working as desired by the State.

15.0 Management and Administrative Control

15.1 Whatever options the State may opt, the overall management control shall be with the State Government both de jure and de facto. The State will be responsible for compliance with all guidelines through its designated Department/Agency. However, appropriate agreements to give effect to this, may be worked out between the State and the outsourced vendor wherever required.